SECURITY AT LAWRENCE LIVERMORE NATIONAL LABORATORY

Hearing of the U.S. Senate Committee on Energy and Natural Resources
May 5, 1999

C. Bruce Tarter, Director
Lawrence Livermore National Laboratory
University of California

OPENING REMARKS

Mr. Chairman and members of the committee, I am the Director of the Lawrence Livermore National Laboratory (LLNL). Our Laboratory was founded in 1952 as a nuclear weapons laboratory, and national security continues to be our central mission. Livermore is a principal participant in the Department of Energy's Stockpile Stewardship Program, heavily involved in programs to prevent the proliferation of weapons of mass destruction, and engaged in energy, environmental, and bioscience R&D as well as industrial applications of our core technologies.

We take security very seriously at Livermore. An extensive security apparatus is in place at our Laboratory, and we continually make adjustments and upgrades to address new threats and concerns. We take strong positive action on counterintelligence issues, whether they are anticipated or identified by us or raised by executive or departmental orders. Today, I would like to discuss this triad of security—physical, cyber, and counterintelligence—and its application at Livermore.

PHYSICAL SECURITY AT LIVERMORE

Livermore's security construct is based on a series of defensive layers—a graded approach that provides increasing barriers that correspond to the increasing value of critical Laboratory assets.

Clearances, badging, and background checks on Laboratory employees (including subcontractors) constitute a first line of defense. Those people with access to the highest levels of classified assets undergo background investigations associated with DOE Q and L clearances and sensitive compartmented information (SCI). Reinvestigations are scheduled automatically at five-year intervals or as needed on a for-cause basis.

Livermore uses a defense-in-depth approach to physical barriers—fences, doors, repositories, and vaults. The Laboratory's outer perimeter fence provides the basic physical protection to U.S. government property. Additional protection is provided for "limited" areas where classified assets are present. The level of clearance required to freely transit these areas is also higher. Classified parts and materials are provided additional physical protection and access control. Significant quantities of special nuclear material receive the highest level of protection, with vault-like physical protection as well as aggressive armed defense and response capabilities.

At each physical barrier (e.g., fence, building, vault), there are various levels of access control. Security officers check badges and in more restricted areas, they check people against specific access lists; at unmanned security portals, badges are checked against access lists. Need-to-know is required, in addition to the appropriate clearance, before an individual is allowed access to classified assets.

The Laboratory employs security officers who are fully trained and accredited. The level of training varies with the assignment (defensive, offensive, or special response). Training is extensive and performance-based. The security force undergoes regular performance tests, self-assessments, DOE surveillance, and inspections.

Physical security is designed into new facilities and facility modifications. Detection systems are continuously monitored and routinely tested. The Laboratory's security system is prepared for armed response to all unauthorized intrusions.

Although Livermore recently received a "marginal" rating in safeguards and security, this assessment reflected a deficiency in procedures. The specific concern involved our inability to meet inventory monitoring requirements because the Plutonium Facility was shut down to address safety concerns, preventing monitoring and measurements. Now that safety concerns have been addressed and the facility reopened, we have resumed all special nuclear material measurements and inventory monitoring and we believe we are now compliant with DOE requirements.

We have high confidence in our Safeguards and Security programs and in the security of our critical assets. We have implemented technical and procedural enhancements to strengthen our physical security, remedied material control and accounting deficiencies, and revised our strategy to protect nuclear material at our Laboratory (including the deployment of a Special Response Team).

CYBER SECURITY AT LIVERMORE

Cyber or computer security is a critical element of Livermore's overall security construct. The Laboratory has both classified computer networks and unclassified computer networks. The two are separate and are not connected. We also have numerous stand-alone computer systems and local area networks in both classified and unclassified areas. There are no connections from Livermore's classified computers to the outside world except through NSA-approved encryption.

In addition to physical barriers between the unclassified and classified computing environments at Livermore, there are need-to-know barriers within the classified computer systems. Access to a classified computing network does not grant users access to all the information in that network. The same need-to-know requirements that apply to verbally communicated information and documents also apply to computer-stored information.

Recent concerns about espionage involving computer-based information and codes spurred a thorough reassessment of computer security at our Laboratory, including threat awareness and training. We support the Secretary of Energy's cyber security initiative and are contributing to his INFOSEC planning.

On April 2, 1999, the Secretary of Energy called for a stand-down of all classified computing at the three DOE national security laboratories. At Livermore, we went even further and shut down all classified computing, all co-located unclassified computing, and all unclassified supercomputing.

We took dramatic steps to focus the attention of all Laboratory employees on the threat of foreign intelligence sources as related to cyber security. All employees (including those who do not normally use computers but could have need or access in the future) received special computer security training. We also trained subcontract employees and consultants. All computing was discontinued until training was complete for all employees on site. Employees who were on travel or leave were trained immediately upon their return.

Every computer work area and environment at Livermore was evaluated and changes were made as necessary to ensure that LLNL classified and sensitive computing meet the highest standards of information security. We have also taken measures to preclude the transfer of information from classified to unclassified computers in a single work area by the use of removable media. We have instituted two-person controls over the authorized transfer of unclassified information from classified computers to unclassified computers. We also have begun to scan outgoing presumably unclassified e-mail for sensitive or classified information.

Although we have strong need-to-know controls on our classified network, we are investigating ways to provide an even greater level of protection. We are also studying how to apply these same concepts to the unclassified systems to provide better protection to unclassified sensitive information.

On our unclassified computing network, we are improving the way we protect unclassified sensitive information. Some information must be available worldwide, but other information must be protected for privacy, proprietary, or export control reasons. We are implementing additional “firewalls” within our unclassified network to separate fully accessible information from unclassified sensitive information

Our approach to cyber security goes beyond addressing vulnerabilities or problems that we identify or that are brought to our attention. We are using this cyber security upgrade as an opportunity to apply our multi-disciplinary approach to science and technology to become a model for cyber security. Leading-edge cyber security is vital to our programmatic missions and is an area where we can leverage our expertise to enhance national security in the broadest sense.

LIVERMORE’S COUNTERINTELLIGENCE PROGRAM

Livermore’s formal counterintelligence program (Security Awareness for Employees, or SAFE) was established in January 1986 in response to a Presidential Decision Directive dated November 1, 1985, that required all U.S. government agencies to establish their own counterintelligence programs. The impetus for the directive was a number of cases in the 1980s of U.S. citizens spying against the United States. (Prior to this time, Livermore addressed counterintelligence concerns through cooperation with the local FBI office, including joint work of mutual benefit and regular discussions on how to reduce the threat of espionage.)

SAFE’s purpose is to identify and counter foreign intelligence threats against Laboratory personnel, information, and technologies. Central to this effort is employee awareness about counterintelligence issues. SAFE provides briefings and debriefings for personnel who host foreign visitors or travel abroad as well as presentations on espionage-related topics by guest speakers from the U.S. intelligence community. These activities help employees recognize if they are the subject of espionage recruitment or information collection efforts by foreign agents and teach them what to do in such a situation. SAFE also provides a consistent way of checking the backgrounds of all foreign contacts.

Livermore notifies the U.S. Department of Energy (DOE) Office of Counterintelligence of all proposed visits or assignments of sensitive country foreign nationals to the Laboratory, so that that office, can request necessary background checks. SAFE also notifies the local FBI field office of proposed visits by foreign nationals from Russia or China. In addition to the pre-travel and pre-visit briefings required by DOE Orders, SAFE also debriefs Laboratory travelers and hosts at the conclusion of their foreign travel or foreign national visit. The information gathered from these debriefings is shared with the U.S. intelligence community, providing valuable input regarding the continually evolving espionage threat as well as feedback on the effectiveness of SAFE's counterintelligence efforts.

History of the SAFE Program

During SAFE's early years, we took a number of steps to align our counterintelligence program closely to the FBI model. By the mid-1990s, SAFE was functioning effectively at LLNL and was well integrated into the U.S. counterintelligence community.

In the early 1990s, in response to the Laboratory's growing number of foreign interactions, particularly lab-to-lab programs, SAFE hired several analysts from the U.S. counterintelligence community. In 1992 a former CIA foreign intelligence analyst and Russia expert was hired, and in 1993 a former FBI Special Agent supervisor and China expert was brought in to manage the SAFE program. Another former FBI China expert was hired in 1994, and a former FBI Middle East and counterterrorism expert was brought on board in 1997. This week, another former FBI China expert was added to SAFE's staff.

Over the years, SAFE has increased the depth and specificity of its briefings for Laboratory employees embarking on foreign travel or hosting foreign visitors or assignees. SAFE reviews the proposed travel or visit, taking into consideration such factors as the foreign country involved, the length of stay, the subject matter to be discussed or studied, the specific facilities or areas to be visited (in the foreign country or at Livermore), and applicable U.S. or foreign government restrictions. If necessary, SAFE works with the traveler or host to modify the travel or visit.

In August 1996, we took another step to augment counterintelligence related to foreign travel and foreign national visitors. Our Proliferation Prevention and Arms Control Program took on the technical review of all requests for travel to sensitive countries by Laboratory employees and all visits and assignments to the Laboratory by foreign nationals from the former Soviet Union, Middle East, Eastern Europe, South Asia, and the Pacific Rim. These reviews focus on the technical content of the proposed travel or visit as it relates to the likely benefits to the foreign country's weapons programs and the concomitant risks posed to U.S. national security.

Response to Curtis Tasking

In November 1996, DOE Deputy Secretary Curtis met with the Directors of the Los Alamos, Lawrence Livermore, Sandia, Oak Ridge, and Pacific Northwest National Laboratories to address the foreign visits and assignments programs at those laboratories. Three taskings specific to the laboratories resulted from this meeting: conducting foreign intelligence threat assessments at each lab, developing a new database to track foreign visits and assignments, and updating the sensitive unclassified topics list.

At Livermore, a Foreign Interactions Day was held in December 1996 in which senior Laboratory managers laid out plans for meeting these Curtis initiatives. Livermore's selfassessment of the threat posed by foreign intelligence collection efforts was launched immediately. Our threat assessment was conducted with assistance from DOE's counterintelligence program (NN-30), and a report documenting our findings was provided to DOE in April 1997.

In March 1997, Livermore hosted a DOE-wide workshop to design an improved database for tracking foreign visits and assignments. The initial idea was for a system that could be used by all the DOE laboratories. In April, we submitted a proposal for a DOE-wide database to track foreign visits and assignments. When DOE declined to adopt a single database design for use by all the laboratories, we went on to design, develop, test, and implement the Visitor Tracking System for use at Livermore. As of May 3, 1999, this system is functional across the Laboratory. Information on each foreign visit and assignment is entered into the system as part of the review and approval process. The database automatically captures numerous pieces of information about each visit and assignment and can provide statistics as needed for periodic reviews and for refined management of the foreign visit and assignment program.

The technical content of proposed foreign visits and assignments is evaluated against a list of sensitive unclassified topics. The purpose of this list is to identify those unclassified topics and technologies that potentially include sensitive information that can be disseminated only after careful review of the specific topic and recipient. Sensitive information is information for which disclosure, loss, misuse, alteration, or destruction could adversely affect national security or federal government interests. Defining sensitive unclassified topics and technologies is a difficult and complex task. Such a list must be used as an indicator that careful attention is required, not as a mechanism for automatic decisions on access. Sound technical judgment must be applied, using the list as guidance, to make a reasoned weighing of proliferation and national security concerns vis a vis the value of scientific interactions.

Livermore's sensitive unclassified topics list, initially drawn up in 1995, is available for reference on the Laboratory's internal web site. Although no DOE Headquarters-led effort for a department-wide update of the sensitive unclassified topics list materialized after the November 1996 Curtis meeting, we have had an ongoing effort at Livermore to keep current our critical and sensitive information list (CSIL; a classified compilation). This list is updated annually through the Laboratory's Operational Security (OPSEC) committee. Most recently, in early April 1999, we convened a team of senior Laboratory managers and scientists to rethink the sensitive unclassified technologies list. This group coordinated its efforts with similar teams at Los Alamos and Sandia. Livermore's draft list of sensitive unclassified technical information was completed April 30, 1999, and has been sent to the Director of DOE's Office of Counterintelligence for review and comment.

We have taken other counterintelligence measures related to but independent of the Curtis initiatives. We made a number of changes to our foreign visits and assignments program to provide better control and tracking, including a more restrictive badging policy for foreign visitors (effective March 1997). We now include several senior Laboratory mangers in the review and approval process for foreign visits and assignments, which helps give Laboratory management a better understanding of the counterintelligence concerns surrounding these visits and assignments.

In early 1998, we drafted an export control guide to assist Laboratory participants in the DOE Materials Protection, Control, and Accounting (MPC&A) program and other activities involving collaborations with Russian and former Soviet scientists. Later that year, we revised that guide and incorporated export control guidance from other programs to produce a comprehensive Laboratory-wide guide to export control. We coordinated our effort with our counterparts at Los Alamos and Sandia to ensure that all three laboratories are operating under consistent export control guidance. This document is at the printer and will be available for distribution in mid-May 1999; it will also be accessible electronically on our internal web site.

Response to PDD 61

Presidential Decision Directive (PDD) 61, issued in February 1998, ordered the DOE to establish a stronger counterintelligence program. In February 1999, the DOE issued its plan for implementing PDD 61. At Livermore, we are moving ahead vigorously with many actions in response to the recommendations in the implementation plan that affect the Laboratory.

The plan's counterintelligence recommendations fall into several broad categories: structure and staffing of the laboratories' counterintelligence programs, liaison with the FBI, counterintelligence and security briefings, insider threats, and foreign national contacts.

The plan calls for counterintelligence programs, within the DOE and at the laboratories, to be separated from their organizations' security departments. Livermore's counterintelligence (SAFE) program meets this recommendation. When it was first established, the SAFE program reported to the Director's Office. Since 1995, the SAFE program has resided in the Nonproliferation, Arms Control, and International Security (NAI) Directorate. The Associate Director for NAI is the Laboratory's Senior Intelligence Officer, and the SAFE program manager has direct access to both the NAI Associate Director and the Laboratory Director.

The plan also calls for the laboratories' counterintelligence programs to be staffed with and managed by experienced counterintelligence personnel and intelligence analysts. Since its inception, our SAFE program has been managed by an experienced former employee of the U.S. intelligence community. SAFE's first program manager was a former CIA counterintelligence specialist. SAFE's current manager is a former FBI Supervisory Special Agent. He is assisted by three former FBI agents and one former CIA case officer. In addition, SAFE is a functional part of the Laboratory's Field Intelligence Element (FIE). SAFE draws heavily and frequently on the Laboratory's intelligence analysts and their expertise in foreign weapons programs; SAFE also employs an analyst (half-time) devoted strictly to counterintelligence issues.

Since the 1970s, our Laboratory has engaged in formal interaction with the FBI on counterintelligence matters. Early in 1996, at our initiative, the FBI placed a liaison agent in the SAFE program. Since the late 1980s, FBI Special Agents in Charge from the San Francisco division have visited Livermore for exchanges of information with senior Laboratory management; the most recent visit took place in March 1999, when Livermore hosted Mr. Bruce Gebhardt, the current Special Agent in Charge.

The DOE plan mandates that counterintelligence and security briefings be tailored to reach all segments of the DOE community. Livermore's counterintelligence and security programs produce high-quality focused briefings for all Laboratory personnel. Livermore employees receive periodic security and counterintelligence awareness briefings. All employees, regardless of clearance level, are required to take an annual security and counterintelligence refresher briefing. SAFE sponsors several counterintelligence awareness briefings each year for Laboratory employees, often by speakers from the U.S. intelligence community. In addition, SAFE gives numerous counterintelligence presentations to groups of employees; many of the unclassified presentations are given to uncleared personnel.

In addressing the need to protect against insider threats, the plan's recommendations focus primarily on the need to expand the DOE's current polygraph program and for the laboratories to establish Personnel Evaluation Boards. At present, Livermore does not have a Personnel Evaluation Board as such. We do however have a formalized process for reviewing cases involving employees being considered for adverse employment actions. The Laboratory's Staff Relations Office oversees this review and evaluation process, working initially with managers in the affected employee's department. A review panel of selected Laboratory managers is convened, and representatives of Human Resources, Office of General Counsel, and Personnel Security are brought in as relevant to the specific case. The panel recommends the action to be taken by the Laboratory, based on numerous criteria present in the matter under review. The SAFE program manager is called by the review panel for consultation should panel members become concerned that actions by an employee are suggestive of espionage activity.

The plan also calls for action regarding foreign national contacts at the laboratories. In December 1998, we completely revised our review and approval process for foreign visits and assignments, particularly with regard to sensitive-country foreign nationals. This layered review involves counterintelligence, security, export control, and nonproliferation as well as several senior Laboratory managers. A sensitive-country foreign visit or assignment is not approved until a background (indices) check has been completed. Livermore's Proliferation Prevention and Arms Control Program also evaluates each proposed foreign visit or assignment against U.S. foreign policy priorities.

In addition to the Visitor Tracking System mentioned above, we also initiated a Foreign National Database Project, under the direction of the SAFE program, to capture all pertinent data on foreign visits and assignments to Livermore that occurred between 1994 and 1998. As part of this effort, each Laboratory directorate is developing its own list of sensitive topics that reflects the technical subject matter that was (or could be in the future) relevant to those foreign visits and assignments.

For many years, Livermore has provided guidance to employees to report any close and continuing contact with foreign nationals from sensitive countries. Guidance from our counterintelligence and security programs is based on requirements in the DOE foreign visits and assignments order as well as other DOE security and counterintelligence orders. This reporting requirement is articulated to Laboratory employees in annual counterintelligence awareness briefings as well as in oral and written counterintelligence briefings to Laboratory hosts of sensitive-country foreign national visitors and assignees. We also provide counterintelligence briefings to employees traveling to sensitive countries. Our goal and practice is to brief and debrief all Livermore employees who serve as hosts to sensitive-country foreign visitors and assignees and all employees who travel to sensitive countries.

CLOSING REMARKS

We have long recognized the inherent challenge involved in protecting national security information while fostering the interchange of ideas required for cutting-edge science and technology. Indeed, the nation's security rests, in very large part, on the technological advances that arise from the world-class R&D conducted at Livermore and the other national security laboratories.

A multi-faceted security apparatus is in place at our Laboratory, including physical security, operational security, personnel security, information security, communications security, cyber security, counterintelligence, and employee security awareness. We continually make adjustments and upgrades to address new threats and concerns. We take strong positive action on security and counterintelligence issues, whether they are anticipated or identified by us or are brought to our attention in the form of executive or departmental orders or inspections. Proactive and effective security and counterintelligence allows us to meet the challenge of ensuring national security while operating in a global world.